INFORMATION SECURITY AWARENESS

Logo

State Seal

State of California
Department of Corrections

INFORMATION

SECURITY

AWARENESS

A HANDBOOK FOR EMPLOYEES

Published by:
Information Security Unit
Office of Compliance
Department of Corrections
State of California

Revision: September 2000

Table of contents

What is this Guide all about?

The purpose of this booklet is to ensure that each employee of the California Department of Corrections (CDC) is aware of his or her responsibilities with respect to Information Privacy and Information Security. As an employee of CDC, you have been trusted with CDC's information. With this trust comes the responsibility and obligation to ensure that the information and computing facilities are used only for their intended business purposes. CDC handles sensitive and confidential information on a daily basis and the responsibility is great.

Take a few moments to review this guide. It will explain what you need to know to be an active participant in CDC's Information Privacy and Information Security Program.

This guide has the following objectives:

- Introduce you to information privacy and information security concepts.
- Provide guidelines on how you can implement information security measures.
- Emphasize the importance of employee awareness in protecting information.
- Make people aware of their responsibilities.

What is information security?

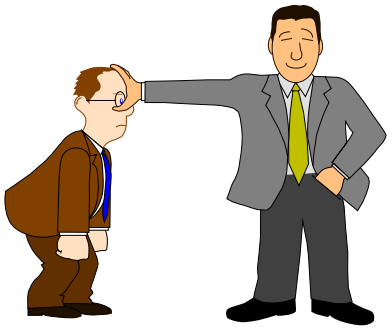
Information security refers to the controls that protect information assets from ***unauthorized*** access, destruction, modification and disclosure. It is a part of your job whenever you work with information to ensure that information is secure. Examples of sensitive or confidential information include personnel files, inmate records, and addresses and home telephone numbers of CDC personnel.

Here are few things you can do:

- Back up information to ensure against loss.
- Lock up diskettes, tapes, or other media when leaving the area.
- Lock doors where appropriate.
- Lock file cabinets that contain sensitive or confidential information.
- Know where the fire exits, alarms, and extinguishers are located.
- Log off you computer when you leave the area.
- Make sure that your computer has current virus protection activated.
- Keep diskettes or magnetic storage media away from magnets, computer tops, or other sources of electrical energy, e.g., coffee pots, hot plates, electric fans, etc.

These are only a few of the things that you need to be aware of, but you get the idea.

What is Information Privacy?



California is one of the few states that provide for the privacy of the individual in its constitution. ***Privacy*** refers to the disclosure of information about an individual while ***security*** refers to the protection of information, facilities, or other assets. Often people think of privacy and security in the same context, that is, if you secure the information you are also protecting its privacy. But it is important to understand that simply disclosing information to a person who is not authorized to receive it is a violation of State and Federal law as well as CDC policy and may lead to adverse action. Information comes in many form, such as:

- Computer screen displays.
- Computer printouts.
- Word processing documents.
- Spreadsheets.
- Graphics and Drawings.
- Presentations.
- Letters, memos and reports.
- Electronic mail and schedules.
- Internet and Intranet.
- Personal computer hard disks and records.
- Floppy diskettes and CDs.
- Microfilm and microfiche.
- FAX documents.
- Conversations both on and off the phone.
- Voice mail messages.

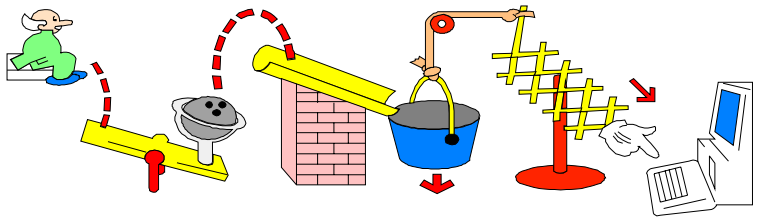
Why should I be concerned about security?

The information that you routinely use may require protection. Whether you work with paper records, on a computer, or spend most of your day on the phone dealing with people, you are an integral part of CDC's information security program. Information security is not an option or choice; **it is a legal requirement**. Information security is embedded in the law and is found in regulatory requirements, in the State Administrative Manual (SAM) Sections 4840–4845, statewide guidelines from the State Department of Information Technology, and is implemented via CDC's departmental policies and procedures contained in the Department Operations Manual (DOM), Volume IV.

What's in it for me?

A lot! If we fail to adequately protect CDC's information from misuse, alteration, or destruction, CDC could not fulfill its mission. Not only does CDC have an obligation to incarcerate California's most serious criminal offenders, it also must protect its employees and those under its care from enduring harassment, injury, or in the worst case, death. You are a part of that process. It is essential that every single employee be an part of the information security program. Examples of incorrectly information or information inappropriately modified:

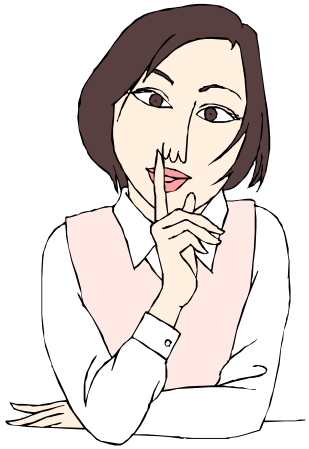
- Incorrect information provided to local law enforcement.
- Release dates calculated incorrectly.
- Wrong medication.
- Incorrect work assignments.



Isn’t security inconvenient?

Some people believe that security means unreasonable controls and that these controls are inconvenient, ineffective, and counterproductive. The reality is that controls and security standards are designed to protect all of us. Appropriate controls and cost-effective safeguards make sure that each person is accountable for his or her actions. Controls protect the honest employee from unwarranted accusations or suspicion. Without accountability, we might all be equally suspect if and when something destructive occurs. Errors or omissions most often cause inaccuracies, lost, or damaged information. With security in place, controls often make it possible to avoid mistakes and omissions, and when they do occur, to identify potential problem areas and limit the extent of damage that mistakes can cause. Security is in place to protect **you** as well as the information and information systems with which you work.

What could really happen?



Even if you aren't responsible for confidential data, information is an asset that must be properly managed and protected. The loss of information can cost time, money and even lives. Incorrect information can lead to all kinds of serious trouble. Here are a few of the things that could happen as a result of poor information security:

- **Loss or Destruction of Information.** It can be difficult, time consuming, and costly to re-create information. In some cases, lost information is impossible to recreate.
- **Unauthorized Access to Information**. CDC's information systems have not only inmate and parolee data, but personal information about employees, such as, addresses and telephone numbers. Disclosure of this information can lead to harassment, physical harm, or even death.
- **Inaccuracies in information.** The vast majority of information maintained by CDC is generated by law enforcement agencies or the courts and must be accurate for the judicial system to function properly. Inaccuracies in information are a serious matter. Inaccuracies can cause delays in legal proceedings, mishandling of information, inappropriate legal actions, mishandling of inmates, or other actions that can have an adverse effect on CDC.

  The department also maintains a large amount information concerning the health of inmates. This information is used to ensure a healthy environment for inmates as well as CDC employees. Health information follows inmates after they are paroled and can effect their return to a normal life. Disclosure, inaccurate or loss of health information can have a negative impact on both inmates and CDC employees.

Are there legal reasons for protecting information?

Yes. California's constitution provides for protect individuals' right to privacy. Additionally, there are Federal and State laws, and a variety of pending legislation making managers and employees legally responsible for the preservation of information integrity and privacy. California has been a pioneer in the development of security and privacy laws. Enacted are provisions that prohibit:

- Violation of copyrights and patents (Federal Copyright Statutes).
- Unauthorized computer access (California Law, 502 of the Penal Code).
- Introduction of malicious computer code such as viruses (California Law, 502 of the Penal Code).
- Causing the unauthorized unavailability of data and/or computer services (California Law, 502 of the Penal Code).
- Unauthorized alteration and/or destruction of data (California Law, 502 of the Penal Code).
- Violation of individuals' Privacy (California Constitution, California Public Records Act (Government Code, Sections 6250–6265)

How can I protect information in my work area?

We tend to become lax about protecting the information in our own work area because we have authorized access to it. We become desensitized to the importance of the information we work with because we see and use it all the time. It is essential that we be alert to the sensitivity of the information and be continually aware of those who may have access to it. It is your responsibility to prevent unauthorized access to CDC information assets by visitors, service personnel, inmates, parolees, CDC employees, or anyone else to whom access has not been granted.

Be aware of how information can be accessed:

- Never share your logon ID or passwords.
- Back up your data regularly.
- Clear your desk at the end of the day.
- Dispose of sensitive documents properly.
- Never discuss confidential information in public areas or with individuals who don't have a need to know.
- Log-off or turn on the screensaver when you leave.
- Challenge unescorted people you do not know.

Be conscious of protecting information:

- Lock up sensitive documents and diskettes.
- Keep food or liquids away from work stations, printers, documents, diskettes, and CD's. Prevent loss of backup diskettes and CDs by storing them away from areas food and liquids.
- Label all diskettes, confidential and sensitive documents appropriately.

But some visitors are OK, right?

Yes, but that doesn't mean that you should allow them to see information that is not intended for their use. Remember, privacy of information is very important. Anyone not currently working in your unit is a visitor. Use caution when disclosing information in the presence of any visitor. This includes:

- Friends and relatives.
- Former and current CDC employees.
- Consultants and contractors.
- Sales and marketing people.

How should I handle questions from outside people?

Depending on your job, you may come into contact with a number of non-CDC people or CDC employees that are not authorized to receive the information that they are asking for. How you handle requests for information depends largely upon who asks the questions. Following are some suggestions:

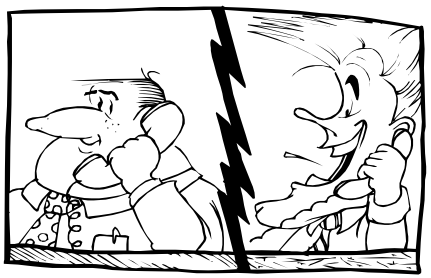
- Verify the identity of the individual asking the questions.
- Refer any requests from the news media (reporters) to the designated Public Information Officer in the CDC Office of Communications.
- If asked to respond to a survey or questionnaire, ask your supervisor if this is acceptable.
- Request for employee information such as lists with home addresses or phone numbers should be referred to your supervisor.

What about phone calls?

When providing information over the phone, it is important to establish the identity of the caller, whether that person has a need to know, and is the caller authorized to receive the requested information. If you have any doubts as to the identity of the individual or his/her right to have the requested information, talk to your supervisor before giving out the information. This is especially important with the increase in *social engineering* incidents. **Do not** give out information to a person who is not authorized to receive it.

Here are some general points to keep in mind:

- Verify the identity of the caller and, if in doubt, say that you will have to call them back, then verify the authenticity with your supervisor.
- Verify their need to know with your supervisor.
- Be aware of social engineering tactics (see section titled *What is Social Engineering*.)
- Verify that the caller is authorized to receive the information.
- Do not give out unnecessary information.
- Be aware of who is in the area around you, and who could overhear your conversation.
- Don't divulge departmental employee information such as lists with home addresses or phone numbers. If you receive a request for this type of information, take the name and telephone number of the individual and notify your supervisor or personnel section.



Are Cell Phones Safe?

No, Cell Phones problems are significantly different that phones in the office. Office phones are in a more controlled environment while cell phones are used everywhere. We use them in the grocery store, airports, and other public areas. We all have the feeling that we must answer the phone no matter where we are, who we are with, or even when a stranger is within hearing. The information we provide over a cell phone is much more public than if we were using the office telephone.

Many of us still use the older analog cell phones which are similar to small two way radios. Anyone with a good radio receiver can listen in on both sides of the conversation. Digital cell phones are a little safer since the signal is converted to digital form. But for both types of phones anyone within hearing can listen to your conversation.

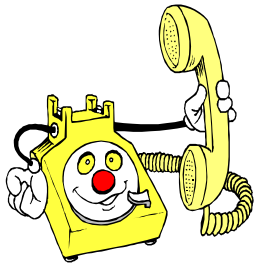
- When using a cell phone be mindful of where you are and who is within hearing distance.
- If you are using an analog phone do not provide sensitive or confidential information. Tell the caller that you will call back when you are in the office. Anyone with a good radio can listen to your conversation.
- If you are in a public area when the cell phone rings ask the calling party to wait while you move to a more private area.
- Be courteous to others, turn off your cell phone or pager , or set the ringer to vibrate when:
  * When in church, a movie theater, or a restaurant.
  * If you are in a restaurant, movie theater, or church step outside to answer you cell phone or respond to a pager call.

Should I be concerned about telephone fraud?

Absolutely! Telephone or toll fraud is one of the fastest growing information security issues today with over $4 billion in loss per year. Losses from prisoners actions nationwide alone exceed $100 million a year. Voice mail, phone card theft, and the transferring of phone numbers or calls are key areas of theft. A popular voice mail scam is to change an outgoing voice mail message to say "Yes operator, I will take that call," or "I will accept those charges." Be aware of anyone near you when using a phone card. Is easy for somebody to steal your phone card number and pin by looking over your shoulder or watching you dial. Lastly, it is extremely important that you protect your voice mail password and privileges.

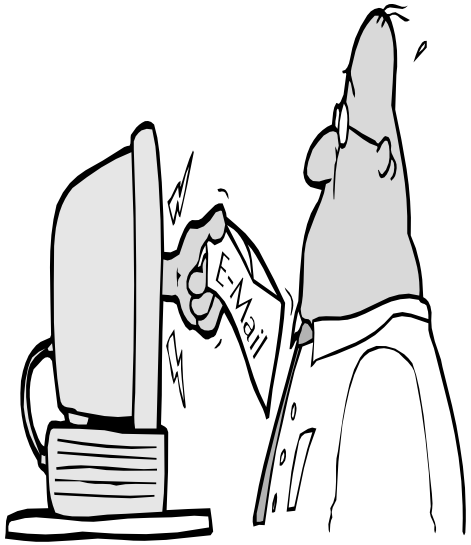
Here are some tips to help you protect CDC's phone system:

- Voice mail passwords should be a minimum of seven characters in length.
- Do not use your phone number in your voice mail password.
- Do not use repeated or consecutive numbers in your voice mail password.
- If your phone has memory capability, ***do not*** program your password into it.
- Follow the password tips provided in "*How can I protect my password?*" in this guide.
- Do not give your password to anyone.
- Remember, telephone service personnel don't need your password to maintain your system.
- If a person who represents themselves to be a telephone service repairman asks for your password they are using social engineering tactics to get the information. Let your supervisor know immediately or call the Information Security Officer.
- Be mindful of "shoulder surfing" when using a phone card.



What about electronic mail?

The State's e-mail system is provided as a tool for State business only. Employees should know that all e-mail messages composed, sent, or received on CDC e-mail systems belong to the Department. CDC has the right to monitor and/or retrieve any e-mail message. You should not expect privacy in your e-mail correspondence.



Here are some guidelines for CDC e-mail users:

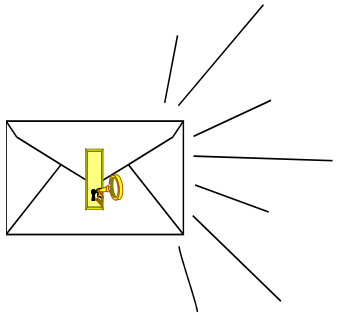
- Use State and CDC e-mail systems only for CDC business purposes.
- Don't send confidential information in e-mail messages.
- Consider the impact of disclosure of the content of an e-mail message before you send it. If the content could be harmful, disruptive, or embarrassing to CDC, the State, public, or yourself—don't send it via e-mail; you might just see your e-mail message appear on the front page of the local newspaper!
- Keep your e-mail password secret just as you would any other password.
- Conduct yourself in a polite and professional manner when sending e-mail messages.
- There is a tendency to think of all mail as being private; It is not! Only mail in the U.S. postal system is considered private. E-mail systems are subject to organizational policy. E-mail sent over the CDC network is subject CDC policy. If e-mail is sent to another department it is also subject to the policies of the receiving department.

E-mail Etiquette

E-mail is unlike other correspondence. With a touch of a button it can be forwarded to hundreds of other people without your knowledge or consent. Everyone that has e-mail has probably had the experience of receiving a memo, joke, or personal note that was funny, offensive, poorly written, or "off the wall." Occasionally, someone will send an organizational memo to the local newspaper to cause embarrassment. E-mail has been used in court cases, as recently happened in a recent antitrust case. E-mail is a good tool with which to communicate but it requires that you use good manners and common sense.

Here are some points to consider when using e-mail:

- Don't send confidential information using email.
- E-mail should be written clearly and to the point. Consider email the same way that you would a memorandum written on paper.
- Know and trust the person you are sending it to.
- Be careful of spelling and syntax. Your e-mail is a reflection of you and your abilities.
- Don't send e-mail messages containing offensive or disruptive information such as sexually-oriented materials or images, racial slurs, gender-specific information, or any comments or images that would offend another individual on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability.
- Don't use all capital letters. It is considered the equivalent of shouting.
- Use appropriate capitalization and punctuation to increase readability.
- Don't use foul language. Keep in mind that your e-mail message may be forwarded to others.



What is social engineering?

S*ocial engineering* is the intentional manipulation of an individual into believing that the caller is authorized and entitled to receive information**.** As the caller makes their way though the organization they gain familiarity with the names, terms, acronyms and jargon, enhancing their credibility as an authorized CDC employee.

Why would someone do this? The simple answer is to gain information concerning your organization. The reasons may not be readily apparent, but can result in serious injury to CDC, staff, or inmates. Avoid being taken in by social engineering:

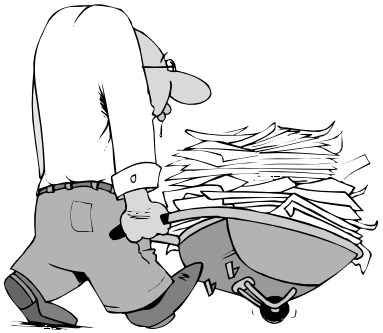
- Don't give out a password over the telephone.
- Don't forward your telephone to a number with which you are unfamiliar.
- Don't mention names of other employees or use CDC terminology unless you are sure of the identity of the caller and their need to know.
- Be especially wary if the caller wants telecommunications information (telephones, modems, voice mail, fax, etc.)
- Don't send documents, plans, schedules, or any other document unless you are sure that the recipient is authorized to receive them.
- If you have any doubts about the caller talk to your supervisor.
- If you have doubts, tell the caller that you will have to call back later and ask for their name and telephone number.
- If you believe that someone is using social engineering tactics to get information notify your supervisor immediately.

What do I do when I want to dispose of sensitive or confidential information?

Confidential and sensitive information are defined in SAM, Section 4841.3 as:

Confidential Information—information maintained by State agencies that is exempt from disclosure under the provisions of the California Public Records Act (Government Code, Sections 6250–6265) or other applicable State or Federal laws; and

Sensitive Information—information maintained by State agencies that requires special precautions to protect it from unauthorized modification or deletion.



Give careful thought before you throw those old pages to procedures, policies, CDC phone directories, etc., in the regular disposal bin. There are people who go through an organization's trash bins looking for information that can be used in gaining access to systems, information or names and acronyms that can in turn be used in a social engineering effort.

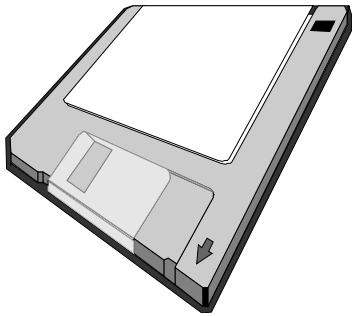
Some suggested methods for disposing of confidential and sensitive material are:

- Use special collection bins designated for confidential destruction.
- Paper shredder.
- Dispose of worn-out diskettes by cutting them in half or breaking them.
- Reformat diskettes or other electronic media prior to giving them to another person. Do not use the quick format option (see section titled *Deleting or destroying confidential data.)* Keep in mind that reformatting does not destroy the information, unless the information is written over the old information still exist diskette or tape.

Deleting
or destroying
confidential Files

Just deleting a file does not mean that the data has been erased from the hard disk or diskette. Keep in mind that although you have deleted the file on your local system it still exists on servers and backup files. When you delete a file(s) just the address of the data is deleted—the data is still there! Using the Windows or NT operating system *quick format* command to erase hard disk or diskettes does not work either, it only erases the data's address. There are a number of software packages on the market designed to retrieve deleted files unless the file has been overwritten. A diskette that contains or once contained confidential or sensitive data must never be passed along unless the entire diskette has be overwritten.

Things to keep in mind when deleting data:



- Deleting a file only removes the file address not the data.
- To delete the data you must overwrite the file, that is, you must write over the files with other characters.
- When sending old computer equipment to surplus or salvage that once contained confidential information, overwrite the hard drive, do a low level format, or physically destroy it.
- To destroy confidential information on diskettes, overwrite the entire diskette. Cutting a diskette in half with scissors will also destroy it.

What about my access to the Internet?

Internet connectivity is provided to CDC employees in order to enhance and facilitate communications, information sharing, and to access research and reference sources. Please keep these guidelines in mind:

- Never leave an active session unattended. If you leave your desk, log-off or turn on the password-activated screen saver.
- Use the Internet for business purposes only.
- Access to erotic, sexually oriented, or anti-government sites is prohibited.
- Infringement of any copyright is prohibited.
- Do not download files except from a reputable source. All files received via the Internet must be scanned for viruses.
- Do not download files from any bulletin boards.
- Downloading, uploading, electronic mail messages, or other postings may not contain any of the following:
    * Derogatory comments regarding race, color, religion, sex, age, disability or national origin.
    * Offensive language.
    * Any content prohibited by law or regulation.
    * Software, computer applications, or other tools whose purpose is to break into or circumvent computer and network security.
    * CDC information or statements regarding CDC without prior approval from the Departmental Public Information Officer.

How can my system access be protected when I'm using a terminal?

Use these simple precautions:

- If it has a mechanical lock, use it when you are away from the terminal, and protect the key from use by others.
- Log-off when you leave your immediate work area. Do not leave an unattended session.
- If you see an unattended terminal being used by an unauthorized person notify your supervisor.
- If sensitive information is displayed on the screen, be sure that no one else can see it.
- **Protect your password!** Do not share it with anyone else. If someone else can successfully log on to the system with your User ID and password combination, all activity will be attributed to your User ID. In other words—**YOU.**

What must I do if I want to use State owned equipment for work at home?

Microcomputers may be stolen or damaged when they are removed from the office. If you take equipment home, remember these important points:

- Obtain approval from your manager or supervisor to use State owned equipment away from the office.
- Obtain an equipment pass if your division has such a requirement.
- Use care in handling the equipment.
- Follow CDC's security procedures to protect the equipment from loss or theft.
- Do not leave equipment unattended.
- In public facilities, watch your equipment while making phone calls, using the bathroom, reading a newspaper, etc.
- Don't leave equipment in your car overnight or where it is visible.
- CDC's computer systems, including networks, workstations, software and peripherals, such as, printers, scanners, and modems are to be used only for CDC business. Access to these resources is limited only to those employees engaged in authorized CDC activities. Misuse of these facilities can lead to adverse action.

How can I protect information at home?

The same rules apply at both work and at home. Be sure that you know the classification level of the information and apply the appropriate controls. Be sure that you:

- Lock up information that is not being used.
- Make backup copies of your information and leave them at the office. Protect the information from disclosure, damage, or destruction.
- Protect sensitive/confidential information from casual observation by others. Don't throw confidential or sensitive information in the garbage can. Bring it back to the office work for proper disposal.

Can I bring my home computer to the office?

It is not recommended since the State does not assume liability for personal property brought to the job site.

I use a modem on occasion; should I use any special precautions?

You bet! Using a modem to connect to CDC systems is the same as being connected to the CDC network at the office. The same rules apply as if you were sitting in your work area using a computer. Never leave an active session unattended and be aware of anyone that can see the information on the screen. Other things you can do include:

- Lock up your modem with your computer when not in use. If your modem is on a card in your computer make sure your computer is in a lockable area.
- Do not use a modem on a computer already connected to the CDC network.
- Access reputable sites only.
- Use virus scanning software whenever information is down loaded.
- No modem of any type inside secure perimeter unless authorization is obtained.

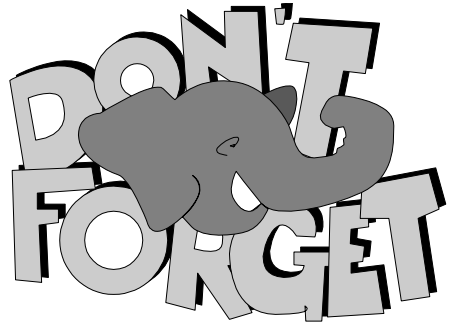
How can I choose passwords that I can remember without writing them down?

The whole idea of a password is to prevent someone from gaining access with your system privileges. Some passwords are easy to guess, especially if the person knows you or if you make the password simple. Try to use words or character strings that mean something only to you. Be sure to include a number(s) or a special character within your password. Here are some suggestions for choosing a GOOD password:

Choose a word that you will easily remember, remove the vowels and insert a number or two, for example:

- PRESIDENT ⇒ PR2SDNT
- Use the first letters in a phrase, for example: The quick brown fox jumped over the ⇒ TQBFJOT
- Combine two misspelled words and insert a number, for example: TRUE BLUE ⇒ TRU7BLU

Just a reminder, don't use these or any other examples provided in awareness materials and training.



Your Password !!!!!

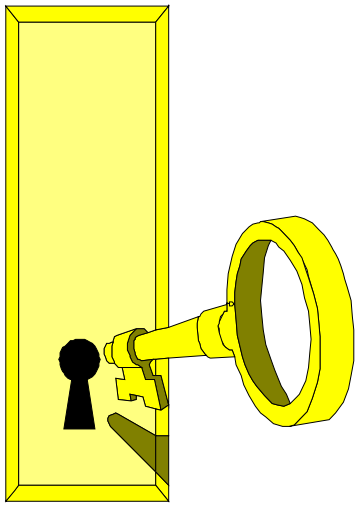
What passwords should I avoid?

Here are some words you should **not** use as a password:

- Your name, nicknames, initials, or names of family and friends.
- Your system User ID.
- Dates; especially those that appear on your driver license or in a personal calendar that you carry in a wallet or purse.
- Telephone numbers, home addresses, zip codes, social security numbers, etc.
- Names of pets, hobbies, special interests, etc.
- Words that appear in any dictionary (they can be compromised by password cracking programs that use electronic dictionaries).
- Consecutive keys on a keyboard, e.g., QWERT or FGHJKL.
- All the same character, e.g., XXXXXX or 999999.
- Default passwords shipped with the system or software.
- Words in which the letter “O” has been replaced with zeros.

How can I protect my password?

First of all, keep in mind that your password controls access to the information contained in the system. The password is for your use only. Giving away your User ID and password is the same as giving someone your bank automated teller card and PIN number. **Remember:** you will be held responsible for all system activity that is associated with your ID and password. You can protect your password from misuse by:



- Changing your password frequently, at least every 90 days.
- Change your password immediately if it becomes known or you suspect it is known by anyone else.
- Select hard-to-guess passwords containing seven or eight characters—but not so hard that you have to write it down to remembered it.
- Enter your password in private with no one in a position to observe your keystrokes (the system should not display the password on the computer screen).
- Do not use words on the "passwords to avoid" section. Do not write down your password on your desk pad, calendar, phone book, address book, etc.
- Do not stick your ID and password on the side of your computer with scotch tape

What about inmates and parolees?

Because inmates work throughout the institutions in many different capacities, it is important to protect not only CDC's information, but also your own personal information. A few precautions you should take are:

- Do not leave confidential, sensitive, or personal information where a curious inmate or parolee can view it.
- Lock up confidential, sensitive, or personal information when you are not in your work area, even if you're just going to be gone for a few minutes.
- Do not dispose of confidential, sensitive, or personal information in a manner that will allow an inmate to remove or view it, such as putting in the trash.
- Do not discuss confidential, sensitive, or personal matters where an inmate or parolee might overhear.
- Be sure that inmates or parolees cannot see the information on your computer screen.

The inmate work force

Inmates are used as a computing resource in cases where it has been determined, via a risk analysis, that the risks are acceptable. However, inmate access to computers must be tightly controlled and closely supervised in these instances. For more detailed information, contact the CDC Information Security Officer for a copy of the pamphlet "Information Security—Inmates and Computers." Review DOM 42020.6 for CDC policy regarding inmate access to computing.

Here are some basic rules for inmate computer usage:

- Inmates with a history of computer fraud or abuse aren't allowed access to computers.
- Inmates are not allowed to use computer-based programming tools which can be used to create or modify computer programs, in addition, they are also not allowed access to computer utility programs such as those produced by Symantec, Norton, or Computer Associates.
- Inmates are only allowed access to a microcomputer to use a specific program.
- All microcomputers used by inmates must be labeled as such and be located in a designated, controlled area which is posted to indicate inmate computer usage.
- Microcomputers that are used by inmates can't be used for any other purpose.
- Inmates are not allowed to have independent storage media (diskettes, tapes, R/W CDs) outside of an approved area.
- Inmates are not allowed to have a microcomputer outside of an approved area or as personal property.

Access to Computers by Inmates in any Capacity

The foremost consideration of CDC is the security of the institutions. The computer's ability to communicate, access, modify or destroy information presents an unacceptable risk to CDC, staff and other inmates. To eliminate or reduce the risk to an acceptable level CDC has restricted the use of computers by inmates. Policies have been developed that prohibit inmate access to computer, modems, or terminals outside of an authorized work or vocational area. For brevity the policies in this awareness booklet paraphrase the policies in DOM. You are encouraged to review the policies DOM section 42020.6.

- Each computer will be labeled to indicate whether inmate access is authorized.
- Areas where inmates are authorized to work with computers will be posted as such.
- No telephones, computer lines, modems, or wireless communications devices will be allowed in areas which inmates have access.
- Utilities that can modify a computers operation, such as, Notons Utilities, or PC Tools, or commands such as DEBUG, ASSIGN, OR ATTRIB will not be made available to any inmate.
- Inmates performing data entry or word processing in an authorized education or work production area will be supervised.
- Inmates who have document sophisticated expertise or histories of computer fraud or abuse will not have duties involving used of personal computers.
- Inmates will not have access to computers containing confidential or sensitive information.

Can I make copies of State-owned software to use on my home computer?

No, unless the software license specifically allows it's use on more than one system and your manager has approved it. Some software companies allow the user to make one copy for use at home. The intent being that when one copy is being used—the other isn't.

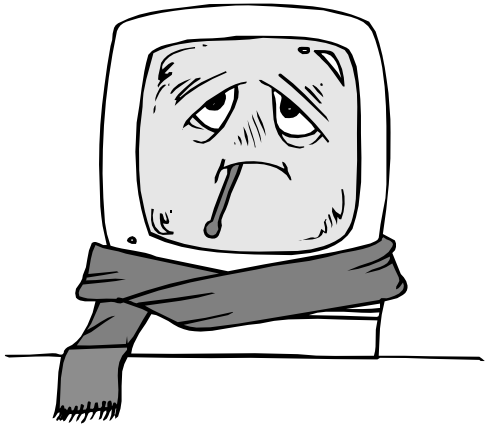
Misuse of State-owned software can expose you and CDC to potential lawsuits for violation of U.S. Copyright law. When the State buys proprietary software, it purchases only a license to use it on a specified number of computers. Making and using copies not authorized under the license agreement is a violation of the law.

I can make a copy of the software I wrote, can't I?

No, State law prohibits employees from "using State time, facilities, equipment, or supplies for personal gain or advantage." Therefore, any software developed on State time, using State equipment, facilities, or supplies, is owned by the State, not the individual responsible for its development.

Should I be concerned about computer viruses?

Yes, concerned enough to take the appropriate precautions. While you might not be able to totally eliminate the possibility of contracting a virus, you can greatly reduce the risk of infection and the potential for serious damage.



- If your computer does not have virus detection software ask your supervisor to purchase some.
- Don't download software from a bulletin board or unknown or "suspect" website.
- Don't bring files from home or anywhere else unless they have been tested for viruses.
- If your computer has been sent out for repair check it with virus detection software before putting into general use.
- Never connect to the Internet unless your virus protection software is active and current.
- Do not open e-mail attachments unless you know and trust the sender. The most damaging virus epidemics have be propagated through the e-mail system.

What steps can I take to reduce the exposure to a computer virus?

There are two simple things you can do to avoid the frustration, cost, and embarrassment of getting a computer virus:

- Back up your system regularly.
- Restrict use to authorized people, reputable software, and verified clean (i.e., virus-scanned) diskettes or CDs.

Here are some specific tips for preventing or lessening the impact of a virus attack:

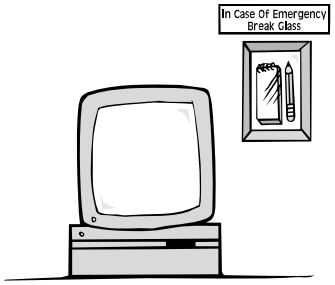
- Use shrink-wrapped software purchased through the State procurement process.
- Make backup copies of all original software diskettes as soon as the package is opened (be sure to use clean virus scanned diskettes.)
- Keep program diskettes *write-protected* whenever possible and store originals in a safe place (e.g., locked cabinet or desk drawer).
- "Shareware" and "freeware" are prime entry points for system viruses. **Do not** use these types of software without management permission. Virus scan before use.
- Be especially cautious of demonstration diskettes, diskettes used on college campuses, and computer technician's diskettes. Because of their exposure to numerous computers, these are major sources of computer viruses.
- Scan all diskettes, including newly purchased shrink-wrapped software, before using them for the first time or if the diskettes were previously used in another computer.
- When downloading a file, download it onto a diskette first and scan it for viruses.
- Make regular backup copies of your files.
- Update your virus software often—new viruses are discovered all the time (most virus software vendors put out updates monthly).

What are the symptoms of a computer virus?

While there are no universal symptoms, here are some things you can look for:

- Programs suddenly take longer to load.
- Disk access seems excessive for simple tasks.
- Unusual error messages appear.
- Access lights come on when no disk activity should occur.
- Less memory is available.
- Files mysteriously disappear.
- Less disk space than normal is available.
- Files change size, date, or content.
- Unexpected messages or characters appear on the screen.

What should I do if I suspect a possible virus?



Stop whatever you are doing on the computer. Report the problem to the Information Systems Branch (ISB) Help Desk if you are at Headquarters. If you are in an institution or parole office, contact the Associate Information Systems Analyst (AISA). Do not attempt to resolve the problem yourself. Prevent access to your computer and diskettes until the problem has been resolved. If indeed it is determined that you do have a virus, all of your diskettes must be scanned because they may also be infected. Install virus protection software.

Should I make backup copies of the data?

Absolutely! Data and other forms of important electronic information should be backed up regularly and stored in a safe place away from your office. Making backup copies can be a real time saver if something happens to your reports, diskettes, and files. Your manager/supervisor should be able to give you more specific guidance on what information should be duplicated and how many copies are needed. This is becoming even more important due to the risks of computer contamination by things like computer viruses. Generally, information must be backed up in multiple copies if:

- You can't afford to lose it.
- It would cost more to re-create it than the cost of backing up.
- It would take too much time to re-create it.
- It can't be re-created because the original source is no longer available.

What are some good backup practices?

Remember that the purpose of multiple backup copies is to replace the original backup copy if something happens to it. Here are some important points to remember:

- Make an extra copy for safety (information on a diskette/tape is usually easier/cheaper to copy and store than paper.)
- Make an extra copy whenever it has changed enough to require a fresh copy (this may be every day or even more often depending on the information.)
- Test your backup software's restore capability—don't assume your backups will work (finding out your backups are bad when you need them is a little too late.)

- Keep more than one generation (i.e., Week 1 Backup, Week 2 Backup, etc.) of backup copies.
- Store your backups in a fire-resistant media safe or far enough away from your work area so that in the event of a fire, flood, earthquake or other event that bars return to your work area, your backups will still be available to you.

What is the key to good information security?

People

Aware employees

YOU!

How can I find out more about information security?

For more detailed information, contact CDC's Information Security Officer who is located in the Office of Compliance, and read the DOM, Sections 48000—49000.

LEGAL REQUIREMENTS AND ADMINISTRATIVE POLICIES

The primary provisions concerning protection and disclosure of information under the control of CDC are found in the State Constitution, Federal and State laws, and State and CDC administrative policies. Brief descriptions of the provisions, and if applicable, the associated penalties for failure to comply, are included in this guide. The primary laws and policies for which descriptions are provided are listed below:

- Constitution of the State of California
- Information Practices Act of 1977
- California Public Records Act
- State Records Management Act
- Comprehensive Computer Data Access and Fraud Act (Penal Code 502)
- State Administrative Manual
- Federal Copyright Act
- CDC Department Operations Manual

CONSTITUTION OF THE STATE OF CALIFORNIA

Article 1, Section 1: "All people are by nature free and independent and have inalienable rights. Among these are... ***privacy***."

INFORMATION PRACTICES ACT

The Information Practices Act declares "that the right to privacy is a personal and fundamental right protected by Section 1 of Article 1 of the Constitution of California and by the United States Constitution and that all individuals have the right of privacy in information pertaining to them." In recognition of the fact that privacy is being threatened by careless handling of personal information and the increasing use of computers and other information automation, requirements have been

placed on the maintenance and release of personal information. Following are those requirements that may be relevant to you as a CDC employee:

- Individuals shall have access to records that contain personal information about them.
- Only personal or confidential information that is relevant and necessary to accomplish an agency's purpose shall be collected and maintained.
- Personal or confidential information, as much as is practical, shall be collected directly from the individual.
- The original source of personal or confidential information must be kept, except when the source is the individual, or when a copy of the original is provided to the individual.
- Data collection forms must contain all pertinent details about the information collection, such as agency information, purpose of collection, consequences of not providing the information, any known or foreseeable disclosure of the information, and the person's right to access the information.
- The accuracy, relevance, timeliness, and completeness of the information must be maintained.
- Personal or confidential information should not be disclosed, except to the individual to whom it pertains; with prior written consent of the individual; to employees with a valid CDC business need; or to other governmental entities in compliance with the law.

Individuals who believe their privacy rights have been violated can bring a civil action (lawsuit) against the agency believed to be in violation. Agency officers and employees who are found to have intentionally committed a violation are subject to disciplinary action that may include dismissal. Any person found guilty of obtaining information under false pretences can be charged with a misdemeanor and be fined up to $5,000 or be put in jail for up to one year, or both.

California Public Records Act

Every person has the right to inspect any *public* record. Agencies may establish written procedures for access to the public records for which they have responsibility.

State Records Management Act

Each agency is required to establish and maintain a program for the economical and efficient management of its records and information collection practices.

Comprehensive Computer Data Access and Fraud Act

Penal Code 502 was enacted to protect individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to computer data and computer systems. Following are the basic offenses covered:

- Knowingly accessing and without permission, altering, damaging, deleting, destroying, or using any data, computer, computer system, or computer network for the purpose of planning and/or executing fraud or extortion.
- Knowingly accessing and without permission, taking copies or using data from a computer, computer system, or computer network or taking copies of any supporting documentation.
- Knowingly and without permission, using or causing to be used computer services.
- Knowingly accessing and without permission, adding, altering, damaging, deleting, or destroying any data, computer software, or computer programs.
- Knowingly and without permission, disrupting or causing a disruption of computer services, or denying or causing the denial of computer services to an authorized user.
- Knowingly and without permission, providing or assisting in providing a means of accessing or causing access to a computer, computer system, computer network.

The penalties under this law range from probation to up to three years in prison, with fines of up to $10,000, depending on the severity of the offence and the monetary loss incurred.

STATE ADMINISTRATIVE MANUAL

The SAM requires that agencies provide for the integrity and security of their automated information. This includes information classification, establishing information ownership, establishing a Risk Management process, identification of agency critical applications, development of an Operational Recovery Plan for recovery of critical applications, and reporting of security incidents to the Department of Information Technology.

Should any audit indicate that the State's security policies are not implemented, or that the Department has not taken corrective action with respect to security deficiencies, the Department may be subject to any or all of the following:

- further audit and review by the DOF, Financial Performance Accountability Unit.
- Revocation, by DOIT, of delegated approval authority for information technology projects.
- Application of penalties specified in Government Code, Section 1222.

FEDERAL COPYRIGHT ACT

The Federal Copyright Act, U.S. Code, Title 17, states that persons who purchase software do not have the right to make additional copies without the permission of the copyright owner, except to make another copy for backup purposes.

Criminal Penalties for Copyright Infringement, U.S. Code, Title 18, states that whether or not the individual knew it was illegal, the penalties are:

- *Liability* for damages suffered by the copyright owner plus any profits attributable to the infringement.
- *Statutory damages* of up to $100,000 for each work copied (infringed).
- If the infringement was done "willfully and for purposes of commercial advantage or private financial gain," *criminal penalties* include fines of up to $250,000 and jail terms of up to five years.

CDC's policy is to protect its information from unauthorized modification, deletion, or disclosure. The purpose of this policy is to establish a standard of due care to prevent misuse or loss of CDC's information assets. This policy establishes internal policies and procedures that:

- Establish and maintain management and staff accountability for protection of CDC's information assets.
- Establish and maintain processes for the analysis of risks to CDC's information assets.
- Establish and maintain cost-effective risk management processes.
- Protect CDC employees, who are authorized to access CDC's information assets, from temptation, coercion, and threat.

This guide covers the basics of the CDC information security policies and procedures, you should review the DOM, Sections 48000–49000 to ensure that you have a complete understanding of the Department's information security requirements.

All violation**s **of security policies or procedures are subject to disciplinary action. The specific disciplinary action that will be taken depends upon the nature of the violation and impact of the violation on CDC's information assets and related facilities.

Following is a partial list of possible disciplinary actions:

- Written reprimand.
- Suspension without pay.
- Reduction in pay.
- Demotion.
- Dismissal.
- Criminal prosecution (misdemeanor/felony, State or Federal).

During the time that a suspected violation is under investigation, the suspected violator's access privileges may be revoked or other appropriate action taken to prevent harm to CDC.

GLOSSARY

Accountability: The ability to trace violations or attempted violations of system security to the individual(s) responsible.

Audit Trail: A chronological record of activities that, collectively, provides documentary evidence of the actions taken against information (records/documents.)

Authorized Access*:* Access to information, regardless of media type (paper, electronic, film, etc.), which is granted to specified individuals by management for the purpose of performing specific CDC work functions.

Availability*:* The condition in which information, computer equipment, or computer services are accessible and can be used when needed.

Backup: The duplication of computer programs and files (usually to diskette or tape), prior to any loss or damage to such information, so that the information can be restored in the event the original is destroyed.

Backup Copies*:* More than one copy of programs and files, usually on diskette or tape, used to restore such information if the original is destroyed.

Classification*:* The assignment of information, including paper documents, to a category on the basis of its sensitivity concerning disclosure, modification, or destruction.

Confidential Information: Information maintained by State agencies that is exempt from disclosure under provisions of the California Public Records Act (Government Code, Sections 6250–6265), or other applicable State and Federal laws. See State Administrative Manual (SAM), Section 4841.3.

Confidential information is so defined because its unauthorized disclosure could cause harm to an individual or organization or would be violating an individual's or organizations right to privacy.

Personal information, including personnel, medical, or similar files the disclosure of which would constitute an invasion of personal privacy should be treated as confidential.

All information pertaining to information security incidents and all incident reports are classified confidential and are subject to all requirements for maintaining confidentiality.

Controls*:* Technological mechanisms and/or procedural measures that help enforce information security policies, standards, and laws.

Copyright Law: Software is protected by the Federal Copyright Act, U.S. Code, Title 17–18, which gives the owner of the copyright "*the exclusive rights* to *reproduce the copyrighted work and to distribute copies*." The act of illegally copying software is commonly known as "software piracy."

Critical Application: An application (program(s)) so important to CDC that its loss or unavailability is unacceptable. With a critical application, even short-term unavailability of the services and/or information provided, would have a significant negative impact on the health and safety of the public or employees, the financial or legal integrity of CDC operations, or the continuation of essential CDC programs. All CDC department-wide information systems are considered critical applications.

Data: A representation of information, knowledge, facts, concepts, computer software, computer programs, or instructions. Data may be in any form, for example in storage media, such as, the memory of a computer, in transit, such as, information sent over communication lines, as presented on a display device, such as, a terminal, or in a paper document.

Downloading: The transfer of information from a higher level of a more centralized computer system, such as a mainframe computer, to a local computing configuration, such as, a microcomputer or Local Area Network (LAN.)

Dumpster Diver: Someone who goes through an organization's trash in search of access codes, credit card numbers, computer printouts, and other information that can be used for dishonest purposes.

Electronic Mail: An electronic mail (e-mail) system which allows a person to type a message at one computer or terminal and send that message to someone on another computer or terminal. The message is stored until the receiver chooses to read it.

Electronic Storage Media*:* Media used to store information electronically, such as hard disks, diskettes, and tapes.

Freeware: Software (programs) that is available to anyone free of charge (no licensing fee.)

Firewall: A firewall is hardware and/or software boundary that prevents unauthorized users from accessing restricted files on a network. The part of the network that is not behind the firewall is available to whoever logs on. There are three standard firewall architectures: the dual-host gateway, the screened-host firewall system, and the demilitarized zone firewall.

Hacker*:* A person who gains, or attempts to gain, unauthorized access to computers, computerized information, or software, usually from a remote site.

HUB: Like the hub of a wheel, a central device that connects several computers together or several networks together. A passive hub may simply forward messages; an active hub, or repeater, amplifies or refreshes the stream of data, which otherwise would deteriorate over a long distance.

Information Assets*:* All types of information including, but not limited to, documents, records, files, databases, and information technology facilities, as well as equipment and software owned or leased by the agency.

Information Custodian: An organization (Information Systems Branch) or a service provider (data center) entrusted with the maintenance and processing an agency's automated information. The Information Custodian is responsibility for complying with applicable law, administrative policy, and any additional security policies and procedures established by the information owner; advising the information owner and agency Information Security Officer of vulnerabilities or threats to the information and measures to counter those vulnerabilities; and notifying the information owner and Information Security Officer of any actual or attempted violations of security policies, practices, or procedures.

Information Owner: The individual assigned decision-making authority for specific automated files and databases. The Information Owner has responsibility for classifying the information for which they are responsible, authorizing access to

such information, monitoring and ensuring compliance with agency and State security policies and procedures concerning the information, identifying the acceptable level of risk for each file and database, and defining precautions for protecting the information.

Information Security*:* The protection of information assets against unauthorized access (accidental or intentional), modification, destruction, disclosure, or the inability to process that information (unavailability.)

Information Security Incident: An occurrence involving CDC information assets which violates Federal or State information security laws or State or CDC information security policies or procedures. Information Security Incidents involve the unauthorized or accidental modification, distribution, or misuse of, disclosure from, or access to CDC information assets. Refer to the CDC Handling and Reporting of Information Security Incidents handbook for details.

Information Security Incident Report: A report documenting the details of an occurrence involving CDC information assets which violates Federal or State information security laws or State or CDC information security policies or procedures. Certain types of incidents are reportable to the Department of Finance (DOF), Technology Investment Review Unit (TIRU), require the signature of the Director and Information Security Officer, and must be submitted to DOF, TIRU within ten working days of the discovery of one or more of the following occurrences:

1) Unauthorized intentional release, modification, or destruction of confidential or sensitive information, or the theft of such information.

2) Use of a State information asset in the commission of a crime.

3) Tampering, interference, damage, or unauthorized access to computer data and/or computer systems as described in the Comprehensive Computer Data Access and Fraud Act (Penal Code, Section 502.)

4) Intentional noncompliance, by the Information Custodian, with custodial responsibilities as specified in the SAM, Section 4841.6.

5) Intentional damage or destruction of State information assets, or theft of such assets, with an estimated value of $500 or more.

Information Security Officer: The person, designated by the agency director, who is responsible for overseeing the agency's compliance with policies and procedures regarding the security of the agency's information assets. (See Government Code, Section 11771 and SAM, Section 4840.2.)

Information Technology: All computerized and auxiliary automated information handling, including: systems design and analysis, computer programming, information storage and retrieval, voice, video, and data communications, etc.

Information User*:* An individual having specific limited authority from the Information Owner or management to view, change, add to, disseminate, or delete such information. The responsibilities of Information Users are: using State information assets only for State purposes, complying with applicable laws (including copyright and license requirements), administrative policies, any additional security policies and procedures, and notifying the Information Owner and agency Information Security Officer of any actual or attempted violations of information security laws, policies, practices, or procedures.

Integrity: The condition in which data or programs are protected from unauthorized modification.

Intranet: A local area network which may not be connected to the Internet, but which has some similar functions. Some organizations set up World Wide Web servers on their own internal networks so employees have access to the organization's Web documents, and receiving electronic mail, connecting to bulletin board systems, and surfing the Internet.

Internet: A network of networks; a group of networks interconnected via routers. The Internet (with a capital I) is the world's largest internet**.**

Local Area Network (LAN): Two or more microcomputers connected by cable, telephone wire, or other communication facility, at the same site, providing the ability to communicate or to access shared data storage, printers, or other microcomputer commodities.

Logic Bomb*:* A malicious program, similar to a virus, designed to carry out a *usually* destructive mission in response to a trigger event. Unlike a Virus, a Logic Bomb does not replicate itself.

Log Off: The procedure by which a user ends a session with a computer.

Log On*:* The procedure by which a user begins a session with a computer.

Malicious Code: Malicious code is computer instructions, usually in the form of a program, designed to perform undesired changes to the computer system, data, or programs. See Virus definition for more information.

Microcomputer: Any of the general purpose personal computers or workstations used for personal productivity or for resource sharing, such as file storage, printers or communications. A microcomputer normally runs with an operating system such as, NT, Windows the Macintosh operating system, or one of the UNIX systems.

Modem: A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator. Modems are used to connect to the CDC network, sending and receiving electronic mail, connecting to bulletin board systems, and surfing the Internet.

Mission Critical: A process or business function that is critical to an agency's ability to continue to operate and be able to meet its mission.

Monitoring: The process of analyzing, assessing, and reviewing audit trails, and other data gathered, to detect events that may be security violations or that may possibly create a security incident.

Network: A group of interconnected computers, including the hardware and software used to connect them.

Off-site Storage: Keeping backup files off premises in a secured area.

Operational Recovery Plan: A plan that identifies and documents the agency's critical applications, the information assets necessary to those critical applications, and the agency's plans for resuming

operations following a disaster or other interruption of service affecting the critical applications.

Password: A unique word or string of characters used to authenticate (verify) an identity. Usually associated with an User ID. Passwords are confidential and should be kept secret.

Personal Computer*:* A microcomputer configured to be used primarily by one person at a time.

Privacy: The right of individuals and organizations to control the collection, storage, and release of information about themselves.

Process: The work activities that produce products, including the efforts of people and equipment.

Program: The set of instructions by which a computer operates to accomplish a specific task.

Proprietary Software: Software packages which are developed by independent vendors and marketed to users.

Public Information: Any information prepared, owned, used, or retained by a State agency and not exempted specifically from disclosure requirements under the California Public Records Act, Government Code, Sections 6250–6265, or other applicable State or Federal laws.

Risk: The chance that a loss of information assets or breach of security will occur.

Risk Analysis: The process of evaluating 1) the vulnerability of information assets to various threats, 2) the costs or impact of potential losses to the organization, and 3) the options for removing or limiting risks .

Risk Management: The process of taking actions to avoid risk or reduce it to an acceptable level.

Router: Specialized computer(s) that store and forward data packets between networks, first determining all possible paths to the destination address and then picking the best route based on traffic load and number of hops. A router can be a hardware device or a combination of hardware and software..

Sensitive Information: Information maintained by State agencies which requires special precautions to protect it from unauthorized

modification or deletion (SAM, Section 4841.3). Sensitive information may be either public or confidential.

Shareware: Software available either free of charge, or for a small fee, that the user is allowed to evaluate/use for a short period of time (usually 30 days) before deciding whether or not to purchase it.

Shoulder surfing: A term used in describing a telephone fraud technique whereby an individual will simply look over someone's shoulder in order to see and memorize the numbers being entered. More sophisticated techniques include devices such as a video camera, or tape recorder to record the numbers being entered into a telephone. The acquired numbers are then used to place unauthorized calls.

Social Engineering: Posing as an employee, client, service technician, or any other bona fide (genuine) individual to gain information that can be used to break into a computer system or for other dishonest purposes.

Software: Computer program(s) which consist of instructions that perform a specific function such as word processing.

Surfing: By analogy with riding waves in the ocean, traveling from place to place on the Internet. The idea "Internet surfing" may come from "channel surfing" on the television, which means switching from channel to channel looking for something interesting.

Terminal: A computer display device which displays information generated by the computer system.

Threat: Condition, that given the opportunity, could cause a harmful event to occur.

Unauthorized Access: Access to information which is not within the scope of an individual's job duties or without the permission of management and/or the Information Owner.

User ID: The unique identifier assigned to an individual for the purpose of access to a computer system.

Virus: A self-replicating program, usually malicious. A virus has three parts, a replicator, a trigger, and a mission. The replicator makes copies of the virus program so that it can spread. A trigger is an event that will cause the virus to perform the function for which it

was designed, such as a specific date or time. The mission is the function the virus will perform when triggered.

Voice Mail: Telephone answering system that provides the user with such services as, message forwarding, message storage and retrieval, and message notification.

Vulnerability: Susceptibility of an information asset to a specific threat.

Worm: A malicious program, similar to a virus, that replicates itself and carries out a destructive (usually) mission. Unlike a virus, a worm does not require a trigger event.

Write-Protected: Preventing data from being written onto electronic storage media. The write-protect mechanism varies depending on the type of storage media.